DYNAMIC INTRUSION DETECTION FOR COMPUTER SYSTEMS

ABSTRACT

An intrusion detection system monitors for signature events, which are part of base intrusion sets that include signature event counters, signature thresholds, and base actions. Associated with each base intrusion set is an action set including an action counter, an action threshold, and an action variable. The associated action counter is updated when the base action of the base intrusion set is invoked responsive to the count of associated signature events meeting the associated signature threshold. The action counter is compared with an action threshold. If the action counter meets the threshold, the associated action variable is updated. The action variable is then passed to an analysis engine comprising a set of rules, which analyses the action variable either in isolation or together with other action variables associated with other base intrusion sets. According to the analysis, an element of a base intrusion set or an action set may be changed.